Traccia:

Tecniche di scansione con Nmap Si richiede allo studente di effettuare le seguenti scansioni sul target Windows 7:

1. OS fingerprint
2. Syn Scan
3. Version detection

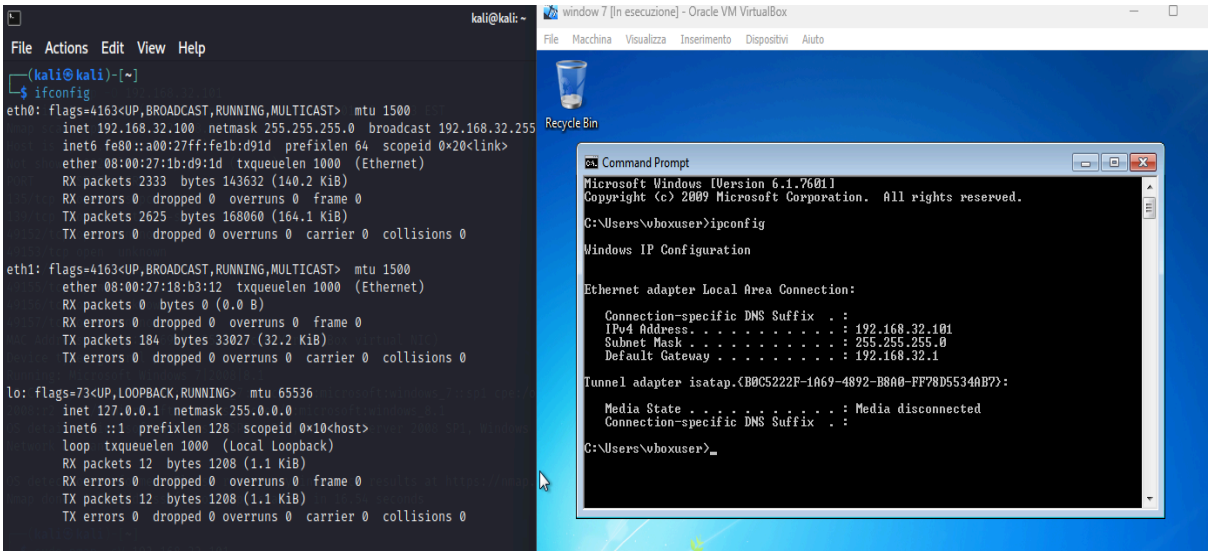
Modificate le impostazioni di rete delle macchine virtuali per fare in modo che i due target siano sulla stessa rete.
A valle delle scansioni, per entrambi gli IP, è prevista la produzione di un report contenente le seguenti info (dove disponibili):

1. IP
2. Sistema Operativo
3. Porte Aperte
4. Servizi in ascolto con versione
5. Descrizione dei servizi

https://www.poftut.com/nmap-output/

nmap -oN report1 IP

Quesito extra (al completamento dei quesiti sopra):
Quale potrebbe essere una valida ragione per spiegare il risultato ottenuto dalla scansione sulla macchina Windows 7? Che tipo di soluzione potreste proporre per continuare le scansioni?



Per prima cosa sono andato a impostare le due macchine sulla stessa rete per far sì che si pingassero.

Scansioni effettuate con nmap:

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.32.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 11:13 EST
Nmap scan report for 192.168.32.101
Host is up (0.00086s latency).
Not shown: 992 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 08:00:27:69:38:55 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_
2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.54 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.32.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 11:21 EST
Nmap scan report for 192.168.32.101
Host is up (0.00077s latency).
Not shown: 992 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:69:38:55 (Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 73.91 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.32.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 11:27 EST
Nmap scan report for 192.168.32.101
Host is up (0.0015s latency).
Not shown: 992 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 08:00:27:69:38:55 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 15.26 seconds
```

Report:

```
┌──(kali㉿kali)-[~]
└─$ cat report2.txt
# Nmap 7.94 scan initiated Fri Jan 19 11:37:58 2024 as: nmap -sV -oN report2.txt -v 192.168.32.101
Nmap scan report for 192.168.32.101
Host is up (0.00074s latency).
Not shown: 992 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:69:38:55 (Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Jan 19 11:39:13 2024 -- 1 IP address (1 host up) scanned in 74.42 seconds
```

Le scansioni effettuate ci suggeriscono che 992 porte tcp non hanno dato riscontro ai test di nmap. Questo probabilmente è avvenuto perché potrebbero esserci delle regole firewall che bloccano il traffico in entrata.

Una soluzione possibile per continuare le scansione potrebbe essere quella di modificare le regole firewall che bloccano il traffico in entrata.